synalyst

SMART NETWORK ANALYSIS

24/7 IT-Security

Monitoring | Analysis
Audit | Troubleshooting
Forensik | Prävention

Synapse Networks GmbH
Peter-Bischof-Straße 2a
55435 Gau-Algesheim
www.synalyst.net
it-security@synalyst.net
0 67 25 999 07 10

Sicherheit durch Analyse

Nur die ständige Analyse des LAN-WAN-Datenverkehrs offenbart Gefahren für Betrieb und Sicherheit und erlaubt vorbeugendes Handeln

24/7 Echtzeit-/Nahzeit-Analyse

synalyst liefert Überwachung der Datenkommunikation im ganzen Unternehmen. Rund um die Uhr, voll automatisiert.

synalyst Analyse liefert
- Speicherung für Forensik
- Tagesberichte
- Monatsberichte
- umgebungsbezogenes Filtern
- Ereignis-Benachrichtigung

synalyst Analyse arbeitet
- non-invasiv (kein aktiver Kontakt)
- keine Perimeter-Verletzung
- Daten-Erfassung via Mirror Port
- software-basierend
- ohne teure Spezial-Hardware

synalyst mit verteilten Analyse-Agenten
- an jedem kritischen Netz-Punkt
- LAN, WAN, Client/Server-Segmente
- vor/hinter Firewalls (trusted/untrusted)
- Campus-Netz und weltweite Netzwerke

Berichte und Benachrichtigungen

synalyst Analyse-Agenten

→
zeichnen den Datenverkehr auf und analysieren ihn sofort nach Speicherung; verwendet wird das offene Libpcap-Format

→
erzeugen umfangreiche Sofort- und Tagesberichte (Logs, Listen, Tabellen)

→
versenden Benachrichtigungen bei kritischen Ereignissen (Syslog, E-Mail)

→
verschiedene Ereignisse können an verschiedene Adressaten gemeldet werden (Techniker, Admins, Vorgesetzte)

synalyst Analyse-Aggregatoren

→
sammeln die Syslog-Meldungen
sammeln die Tagesberichte

→
filtern die Syslog-Event-Logs
filtern die Tagesberichte

→
erzeugen aggregierte Filter-Logs
erzeugen aggregierte Tagesberichte
erzeugen aggregierte Monatsberichte

Praxis-Beispiel: unerkannter Incident

Firewall hält nicht dicht

Firewall sendet interne Daten ins Internet.

Der Admin bestätigt, dass die Firewall auf »blocking« gestellt ist. Der Datenabfluss aber hält an. Der Fall wird an den Hersteller der Firewall eskaliert. Binnen 24 Stunden kommt dessen Antwort:

Die GUI-Beschriftungen für »blocking« und »open« waren vertauscht worden: Wenn der Admin »blocking« anklickte, war der Kanal im Hintergrund »open«.

Da die Firewall daran glaubte, alles richtig zu machen (wie befohlen), konnte sie auch keine Sicherheitsverletzung melden.

Fazit: Die SIEM-Aggregatoren des Kunden konnten folglich keinen Security Event melden, da sie notwendig blind waren.

synalyst Analyse deckt die Gefahr auf.

SIEM allein hilft auch nicht

Das Beispiel zeigt: Ausgerechnet die am meisten kritischen und gefährlichen Ereignisse kommen ggf. erst gar nicht im SIEM an, wenn bzw. weil die aktiven Komponenten die Fehler nicht als solche erkennen und daher nicht melden (nicht melden können).

Überwachung eines weltweiten Daten-Netzes

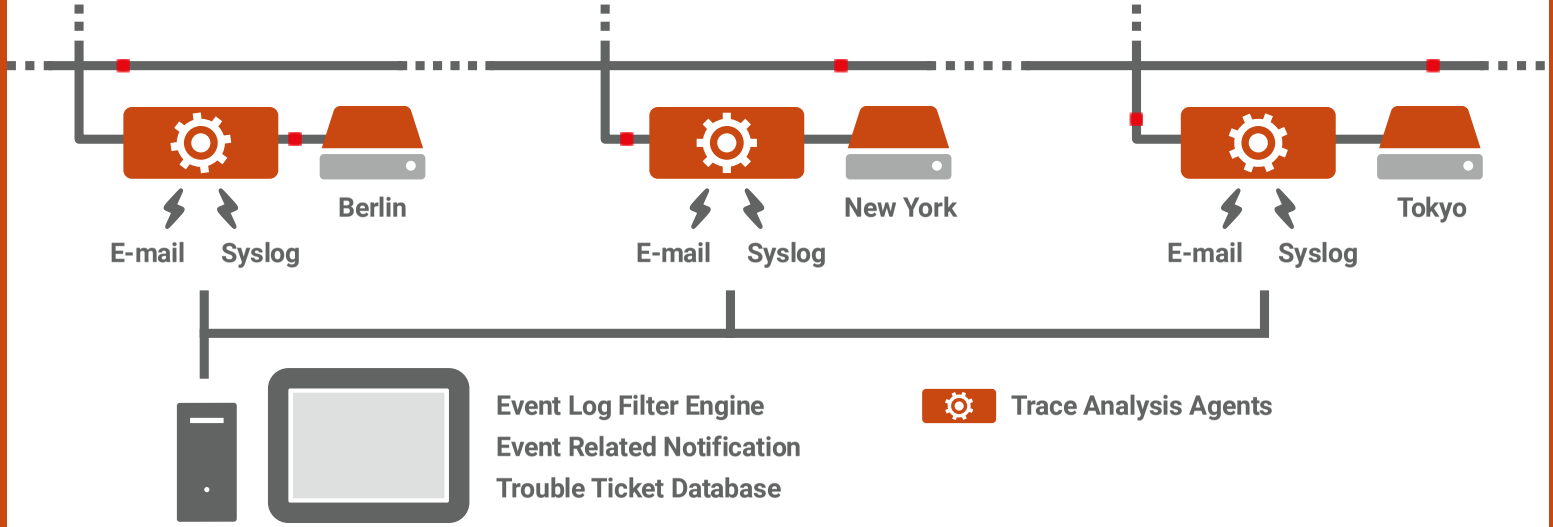
synalyst betreibt für den Kunden:

- 30 Analyse-Agenten weltweit
- 20 Millionen Event-Meldungen täglich (ca.)
- zentrales Sammeln der Events (Syslog)
- Filter-Engine sortiert, priorisiert, meldet
- etwa 600 Filter-Definitionen insgesamt
- etwa 400 davon aktiv
- etwa 200 davon inaktiv (erledigte Fälle); diese werden turnusmäßig zur Absicherung aktiviert, um sicher zu gehen, dass alte Fehler nicht wieder neu aufgetreten sind
- jedem Event können separat definierte Meldungs-Empfänger zugeordnet werden
- Full Managed Service

synalyst Analyse offenbart (Beispiele):

- suspekte Client-zu-Client-Zugriffe
- suspekte Broadcast/Multicast-Versuche
- Jailbreak-Versuche
- Intruder-Vorfälle
- WhiteList-Verletzungen
- Wechsel in Host-ID-Merkmalen
- Wechsel der Routing-Wege
- abgelehnte Logon-Versuche
- DNS/Kerberos/LDAP-Aktivitäten
- Starke Schwankung der Antwortzeiten
- veraltete Logon-Athentifizierung
- veraltete SSL/TLS-Verschlüsselung

synalyst macht sichtbar – sichtbar, was sonst unter dem Radarschirm bliebe



synalyst betreibt für Kunden im Full Managed Service die Überwachung des LAN/WAN-Datenverkehrs.
Insbesondere für KMU und öffentliche Institutionen bieten wir schnelle, angepasste Lösungen.
www.synalyst.net – it-security@synalyst.net – 0 67 25 9 99 07 10
synalyst – Ihr Analyse-Partner in Deutschland und weltweit.

synalyst
SMART NETWORK ANALYSIS